JOINT STATEMENT FOR THE RECORD
OF

JAMES R. CLAPPER
DIRECTOR OF NATIONAL INTELLIGENCE

GENERAL KEITH B. ALEXANDER
DIRECTOR
NATIONAL SECURITY AGENCY
CHIEF
CENTRAL SECURITY SERVICE

JAMES M. COLE
DEPUTY ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE
HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

OCTOBER 29, 2013

Joint Statement for the Record
of

James R. Clapper
Director of National Intelligence

General Keith B. Alexander
Director, National Security Agency and Chief, Central Security Service

James M. Cole
Deputy Attorney General
Department of Justice

Before the
House Permanent Select Committee on Intelligence

October 29, 2013

Thank you for inviting us to discuss the Administration's efforts to enhance public confidence in the important intelligence collection programs that have been the subject of unauthorized disclosures since earlier this year: the collection of bulk telephony metadata under the business records provision found in section 215 of the USA PATRIOT Act, and the targeting of non-U.S. persons overseas under section 702 of FISA. We remain committed, as we review these activities, both to ensuring that we have the authorities we need to collect important foreign intelligence to protect the country from terrorism and other threats to national security, and to protecting privacy and civil liberties in a manner consistent with our values. We also remain

committed to working closely with this Committee as any modifications to these activities are considered. We understand that some of the initiatives announced by the President in his statement on August 9 are of interest to the Committee, and we welcome the opportunity to discuss them with you and to work together in moving forward.

The first step in promoting greater public confidence in these intelligence activities is to provide greater transparency so that the American people understand what the activities are, how they function, and how they are overseen. As you know, many of the reports appearing in the media concerning the scope of the Government's intelligence collection efforts have been inaccurate, including with respect to the collection carried out under sections 215 and 702. In response, the Administration has released substantial information since June to increase transparency and public understanding, while also working to ensure that these releases are consistent with national security.

We have worked to provide the public greater insight into the operation of the bulk telephony metadata business records collection program under section 215. In early June, the Director of National Intelligence (DNI) released a public statement explaining that the program is carried out only pursuant to orders of the Foreign Intelligence Surveillance Court (FISC) and is subject to executive, judicial, and Congressional oversight. The DNI emphasized that, under this program, we do not collect the content of any telephone calls or any information identifying the callers, nor do we collect cell phone locational information. Rather, the Government obtains business records created and retained by telecommunication companies for their own internal purposes, such as billing. The DNI also explained that the Government is authorized to query the bulk metadata only when there is a reasonable, articulable suspicion, based on specific facts,

that the identifier—e.g., a telephone number—used to query the data is associated with a foreign terrorist organization previously approved by the FISC. Subsequently, the DNI declassified and released the FISC's primary order that accompanied the secondary order that had been disclosed in the media, so that the American people could have a more complete picture of the legal parameters under which this activity occurs and the extensive oversight that the FISC requires. The primary order confirms that the Government must adhere to strict limitations on querying, retaining, and disseminating the business records acquired through this program. The Director of NSA also released information concerning the value of the bulk telephony metadata collection program in support of a number of counterterrorism investigations.

In August, the Administration published an extensive white paper to provide more detailed information concerning the section 215 business records program and its legal basis. The white paper explained the process and importance of "contact chaining" under which the NSA may obtain metadata records as many as three "hops" from an identifier associated with a foreign terrorist organization that is used to query the data. It also explained why the telephony metadata collection program meets the "relevance" standard of section 215 and why the program is fully consistent with settled Fourth Amendment law, including the Supreme Court's precedent holding that participants in telephone calls lack a reasonable expectation of privacy in the telephone numbers dialed. Then, in early September the DNI declassified and released more documents concerning the business records program. These documents discuss compliance incidents that were discovered by NSA and DOJ four years ago, reported to the FISC and to the intelligence and judiciary committees, and subsequently resolved. These materials (and others) show that the oversight system worked. The problems were reported to the FISC, the FISC

conducted a rigorous review to ensure compliance with its orders and the protection of Americans' privacy, and the Intelligence Community responded effectively.

We have also substantially increased the transparency of the Government's collection under section 702 of FISA. Even before the recent unauthorized disclosures, the Administration had prepared a public white paper in conjunction with reauthorization of the FISA Amendments Act (FAA) at the end of last year, explaining its intelligence collection activities under the FAA and focusing in particular on collection under section 702. That paper emphasized that section 702 collection targets only non-U.S. persons overseas, and that targeting and minimization procedures and acquisition guidelines are required to ensure that the statutory restrictions are followed and to govern the handling of any U.S. person information that may be incidentally acquired. After the unauthorized disclosures concerning section 702 collection, the DNI refuted much of the inaccurate reporting about the program by releasing a public statement making clear that the Government does not have access to communications carried by U.S. electronic communications service providers without appropriate legal authority. Under section 702 such companies are legally required to provide targeted information to the Government only in response to lawful Government directives, which are issued after the FISC examines and approves certifications required under section 702. The DNI's statement also explained that the Government cannot collect information under section 702 unless there is an appropriate and documented foreign intelligence purpose, such as preventing terrorism or weapons of mass destruction proliferation.

In August, the DNI declassified and released three opinions from the FISC concerning the section 702 program. As was the case with the section 215 opinions, these opinions

concerned a significant compliance incident that caused the Court to criticize the manner in which the section 702 program was being carried out. And, similarly, these opinions provide the public with considerable insight into the nature and functioning of section 702 collection, while also displaying the detailed and intricate extent of the FISC's review. Indeed, while the FISA statute describes the basic procedures by which the Intelligence Community seeks various authorizations from the FISC, the opinions released reveal fully the thorough, thoughtful, independent review that the FISC provides.

The Administration has taken other steps toward increasing transparency more generally in the context of intelligence collection. For example, the DNI recently introduced a new website called "IC on the Record," which provides ongoing, direct access to information about the foreign intelligence collection activities carried out by the Intelligence Community. Administration officials have also made a number of important public statements relating to the Government's foreign intelligence collection efforts, including a speech by the General Counsel of the Office of the Director of National Intelligence at the Brookings Institution. Moreover, the Government has permitted companies interested in providing greater transparency as to their role in these programs to release certain aggregate statistics about their cooperation with lawful demands from the Government, in a way that will avoid revealing the Government's intelligence collection capabilities with respect to particular providers or platforms. And of course there have been a number of open hearings before committees of the Congress on these issues.

Overall, this is a lot of activity for three months. As we have worked toward greater transparency, we have been mindful of the need to protect intelligence sources and methods. Unfortunately, because of the unauthorized disclosures, a great deal of information that was

previously classified about these intelligence programs is now in the public domain. These unauthorized disclosures have already caused significant harm to national security, and inaccurate or incomplete press coverage of the unauthorized disclosures has also undermined public confidence in our efforts to protect Americans' privacy. We have to consider these effects as we assess whether additional harm will flow from releasing additional information. There is still substantial information about these activities that can and must remain classified, and we have therefore taken great care to ensure that any documents that are considered for release are carefully reviewed and redacted as appropriate to protect national security. Ultimately, the Government must walk a fine line by disclosing enough information to assure the American public that the Government is acting lawfully but not disclosing so much information that we put the American public in danger.

To complement these transparency efforts, the Administration has taken a series of steps to enhance independent review of U.S. intelligence collection programs. In his August 9 statement, the President noted the importance of the Privacy and Civil Liberties Oversight Board's (PCLOB's) review. PCLOB's statutory mission is "to analyze and review actions the executive branch takes to protect the nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties." PCLOB is taking an active role in reviewing the intelligence activities carried out under sections 215 and 702. The Board has received extensive briefings from Administration officials concerning these activities and visited the NSA. In July PCLOB sponsored a public workshop to hear from expert panels and the public.

In his speech in August, President Obama also announced the establishment of a Review Group on Intelligence and Communications Technologies. The Review Group's task is to advise the President "on how, in light of advancements in technology, the United States can employ its technical collection capabilities in a way that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure." The group is charged with conducting an independent review and will report to the President. Group members have received briefings from Administration officials and have met with privacy and civil liberties experts, as well as information technology companies and experts. The group will also be soliciting public comments. The Review Group has been directed to submit an interim report to the President within 60 days and a final report by the end of the year.

Throughout this period, the FISC has continued to exercise its central oversight role with respect to intelligence collection carried out under FISA. In July, ODNI announced that the FISC had renewed its approval for the section 215 program. In connection with that renewal, the FISC has also publicly released an opinion explaining the legal rationale for its decision.

Moreover, as the President discussed in his August 9 statement, the executive branch stands ready to work with Congress to pursue appropriate reforms to section 215, to discuss certain changes to practice before the FISC to ensure that civil liberties concerns have an independent voice in appropriate cases, and to consider efforts at strengthening the transparency of these and other intelligence activities, all in ways consistent with protecting national security. Regarding section 215, we are open to a number of ideas that have been proposed in various

quarters to address concerns about the business records program. For example, we would consider statutory restrictions on querying the data that are compatible with operational needs, including perhaps greater limits on contact chaining than what the current FISC orders permit. We could also consider a different approach to retention periods for the data—consistent with operational needs—and enhanced oversight and transparency measures, such as annual reporting on the number of identifiers used to query the data. To be clear, we believe the manner in which the bulk telephony metadata collection program has been carried out is lawful, and existing oversight mechanisms protect both privacy and security. However, there are some changes that we believe can be made that would enhance privacy and civil liberties as well as public confidence in the program, consistent with our national security needs.

On the issue of FISC reform, we believe that the *ex parte* nature of proceedings before the FISC is fundamentally sound and has worked well for decades in adjudicating the Government's applications for authority to conduct electronic surveillance or physical searches in the national security context under FISA. However, we understand the concerns that have been raised about the lack of independent views in certain cases, such as cases involving bulk collection, that affect the privacy and civil liberties interests of the American people as a whole. Therefore, we would be open to discussing legislation authorizing the FISC to appoint an *amicus*, at its discretion, in appropriate cases, such as those that present novel and significant questions of law and that involve the acquisition and retention of information concerning a substantial number of U.S. persons. Establishing a mechanism whereby the FISC could solicit independent views of an *amicus* in a subset of cases that raise broader privacy and civil liberties questions, but without compromising classified information, may further assist the Court in

making informed and balanced decisions and may also serve to enhance public confidence in the FISC process.

And with regard to enhancing transparency and accountability, the President has directed that the Intelligence Community declassify and make public as much information as possible about certain sensitive intelligence collection programs, including programs undertaken pursuant to sections 215 and 702, while being mindful of the need to protect sensitive classified intelligence and national security. Consistent with that direction, the DNI has directed the Intelligence Community to release publicly, on an annual basis, aggregate information concerning compulsory legal processes under certain national security authorities. We stand ready to discuss whether legislation would be helpful in advancing the President's objective of ensuring greater transparency for the activities of the Intelligence Community, where consistent with the protection of classified information.

While it is important that we have the aforementioned dialogue about security and civil liberties, we'd also like to take a moment to reiterate some of the comments the President has made about the hard-working men and women of the intelligence community who work every single day to keep us safe because they love this country and believe in its values. These professionals are Americans, too—they come from the same communities, go to the same schools, and care about the same things all Americans do. While the ongoing debate is an important one, and may well result in changes, that dialogue should in no way be perceived as a negative reflection on the dedicated professionals of our Intelligence Community.

We look forward to working with you on these important issues, and we remain grateful for this Committee's support for these particular intelligence collection programs, which we

continue to believe play an important role in our broader foreign intelligence collection efforts. We hope that, with the assistance of this Committee, we can ensure that these programs are on the strongest possible footing, from the perspective of both national security and privacy, so that they will enjoy broader public and Congressional support in the future. Thank you.